

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF TEXAS  
FORT WORTH DIVISION

UNITED STATES OF AMERICA

v.

RICKY MILLER (02)

Criminal No. 4:16-CR-205-O

FACTUAL RESUME

I. PLEA

The defendant, Ricky Miller, is pleading guilty to Count One of the Superseding Information, which charges the defendant with conspiracy to commit fraud and related activity in connection with computers, in violation of 18 U.S.C. § 371 (18 U.S.C. § 1030(a)(4)).

II. PENALTIES

The maximum penalties the Court can impose include:

- a. imprisonment for a period not to exceed five years;
- b. a fine not to exceed \$250,000.00, or twice the pecuniary gain to the defendant or loss to the victim(s), or both such fine and imprisonment;
- c. a term of supervised release not to exceed three years, which may be mandatory under the law and will follow any term of imprisonment. If the defendant violates the conditions of supervised release, the Court may revoke such release term and require that the defendant serve any or all of such term as an additional period of confinement. The effect of a revocation of a term of supervised release is to make the overall period of incarceration longer;
- d. a mandatory special assessment of \$100;
- e. restitution to victims or to the community, which may be mandatory under the law;

- f. costs of incarceration and supervision; and
- g. forfeiture of property.

### III. ELEMENTS OF THE OFFENSE

In order to prove the offense alleged in Count One of the Superseding Information, that is, conspiracy to commit fraud and related activity in connection with computers, in violation of 18 U.S.C. § 371, the government must prove each of the following elements beyond a reasonable doubt:

- First:* That the defendant and at least one other person made an agreement to commit the crime of committing fraud and related activity in connection with computers;
- Second:* That the defendant knew the unlawful purpose of the agreement and joined in it willfully, that is, with the intent to further the unlawful purpose; and
- Third:* That one of the conspirators during the existence of the conspiracy knowingly committed at least one of the overt acts described in the information, in order to accomplish some object or purpose of the conspiracy.

In order to prove the offense of committing fraud and related activity in connection with computers, a violation of 18 U.S.C. § 1030(a)(4), the government must prove each of the following elements beyond a reasonable doubt:

- First:* That the defendant knowingly accessed without authorization a computer used in or affecting interstate or foreign commerce or communication of the United States;
- Second:* That the defendant did so with the intent to defraud;
- Third:* That by accessing the computer without authorization, the defendant furthered the intended fraud;
- Fourth:* That by accessing the computer without authorization, the defendant obtained anything of value; and

*Fifth:* That the total value of the defendant's computer use exceeded \$5,000 during a one-year period.

#### IV. STIPULATED FACTS


From at least the year 2013, and continuing until on or about September 2015, in the Northern District of Texas and elsewhere, the defendant, Ricky Miller, knowingly agreed to join three other individuals to create a group known as RANE Developments LLC (the "RANE Group"), whose sole purpose was to develop a computer program the group referred to as the "FIFA Server Tool Application," "Application," or "App" (hereinafter referred to as the "application") in order to defraud Electronic Arts, Inc. ("EA") by intently accessing a protected computer without authorization to obtain something of value, specifically "FIFA coins," which had a value of more than \$5,000 within a 1-year time period.


As part of the conspiracy to commit fraud, the defendant assisted in creating the application by reverse engineering EA's FIFA video game. The application allowed the RANE Group to fraudulently instruct the servers, belonging to EA, into believing thousands of FIFA matches had been completed in the company's FIFA video game within a matter of seconds. Once EA's servers believed the matches had been completed, the company's servers would credit various accounts maintained by the RANE Group with FIFA coins. The RANE Group would then transfer and sell the FIFA coins to various coin dealers throughout the world.

During the course of the conspiracy, the defendant and the RANE Group continued to develop new methods to circumvent the security measures EA developed.

The defendant and the RANE Group executed their application through a video game console, which they modified to circumvent security protections. Later in the conspiracy, the defendant and the RANE Group developed a method to execute their application through cloud computer servers, which allowed them to run more copies of the software and obtain significantly more FIFA coins.

AGREED TO AND SIGNED this 14 day of October, 2016.

  
RICKY MILLER  
Defendant

  
JASON FREEMAN  
Attorney for the Defendant